REMARKS

This application has been reviewed in light of the Office Action dated March 21, 2007. Claims 1-18 are pending in the application. Claims 1, 8, 11, 13 and 16 have been amended. No new matter has been introduced. The Examiner's reconsideration of the rejection in view of the amendment and the following remarks is respectfully requested.

By the Office Action, claims 1-18 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Applicant Admitted Prior Art (AAPA) in view of U.S. Patent Application No. 2004/025288 to May et al. (hereinafter May).

AAPA describes a broadcast flag (BF) used to identify that video content not be broadcast outside of the receiving devices network. The broadcast flag is employed by a router to drop the packet if the packet is not supposed to be sent outside of the network. In a home network, this technique is not easily employed. The network may or may not have firewalls or routers around it to scan for such flags. Devices on different networks may communicate without going through a router, for example. No mechanism exists for how such a flag could be implemented in a home network to prevent content from being transmitted outside the home network. One proposed solution included using additional flags but even more infrastructure would be needed in such a case.

May is directed to a SONET network employed for routing both voice and data traffic using packets. The packets may include one or more addresses and the packets may be routed to different destinations. May is concerned with efficient usage of network bandwidth.

While this is always a concern, the security features of the present disclosure are not taught or suggested by May.

While May discloses four different multicast transfer methods, these methods consist of different techniques for efficiently routing packets using the bandwidth of the network (see paragraph [0080]). The first method is based upon the destination node/network that will receive the packets. If the node needs the multicast packets, the packets are transferred, otherwise the packets are dropped. The second method is where the source node replicates the packets for distribution to the next node that has subscribed to the multicast. The third method is to reserve a subset of the destination address space for multicasting. In the third method, a node can subscribe to a frame having a particular multicast address. The fourth method uses header concatenation where multiple headers refer to the same packets. The fourth method has frames that are addressed only to the nodes that need them. This saves bandwidth since the broadcast or multicast is not propagated needlessly through the network. The routing of multicast packets through a SONET network does not disclose or suggest the security aspects of the present invention as claimed.

Claim 1 of the present invention now recites, *inter alia*, determining whether the authorization field is indicative of the first or second transport mode by parsing the authorization field at the access device; and inhibiting transmission of the digital signal from the access device to the destination device in response to determining that the authorization field is indicative of the second transport mode and the destination device is outside the network, otherwise, transmitting the digital signal to the destination device.

AAPA and May, taken singly or together, fail to disclose or suggest an authorization field having a first transport mode authorizing distribution of the digital signal outside the network, and of a second transport mode inhibiting distribution of the digital signal outside the network where the authorization field is parsed by the access device and in one mode the access device inhibits transport of the flagged data. The cited combination fails to disclose or suggest at least: determining whether the authorization field is indicative of the first or second transport mode by parsing the authorization field at the access device; and inhibiting transmission of the digital signal from the access device to the destination device in response to determining that the authorization field is indicative of the second transport mode and the destination device is outside the network, otherwise, transmitting the digital signal to the destination device. Such steps are not performed or contemplated by an access device in either of the AAPA and/or in May. Therefore, the cited combination fails to disclose or suggest all of the claimed elements of claim 1.

Claim 11 of the present invention now recites, *inter alia*, an access device including ... a processor for controlling data receiving and transmitting operations of the access device ... ; and data interface means, coupled to the network, for receiving data from devices attached to the network, and for distributing the digital signals on the network, wherein the processor is configured to parse the authorization field at the access device and the processor inhibits transmission of the digital signal on the network from the access device to the destination device in response to a determination that a destination device is outside the network and that the authorization field is indicative of the second transport mode, otherwise, the processor enables transmission of the digital signal on the network.

The cited combination fails to disclose or suggest at least: the processor is configured to parse the authorization field at the access device and the processor inhibits transmission of the digital signal on the network from the access device in response to a determination that a destination device is outside the network and that the authorization field is indicative of the second transport mode. AAPA and/or May do not disclose or suggest an access device that parses an authorization field at the access device and the processor inhibits transmission of the digital signal on the network from the access device. The access device is preferably a consumer electronics device, such as, e.g., TV, DVD player or the like. Nowhere in the cited combination is an access device disclosed or suggested that provides at least the parsing and inhibiting capabilities as set forth in the present claims 1 and 11. Routers are employed for processing packets in both AAPA and May. Further, the security benefits provided by the present invention would not be realized even by combining AAPA and May since individual access devices would not be able to parse authorization information and inhibit the transport from individual access devices as presently set forth in claim 11. Therefore, the cited combination fails to disclose or suggest all of the claimed elements of claim 11.

It is respectfully submitted that claims 1 and 11 are in condition for allowance over the cited combination. Dependent claims 2-10 and 12-18 are also believed to be allowable at least due to their dependencies from claims 1 and 11, respectively. Reconsideration of the rejection is earnestly solicited.

In view of the foregoing amendments and remarks, it is respectfully submitted that all the claims now pending in the application are in condition for allowance. Early and favorable reconsideration of the case is respectfully requested.

Customer No.: 24498
10/517,089
July 16, 2007

Docket No.: PU020274

It is believed that no additional fees or charges are currently due. However, in the event that any additional fees or charges are required at this time in connection with the application, they may be charged to applicant's Deposit Account No. 07-0832

Respectfully submitted,

Thomas Anthony Stahl, et al.

Dated: 7/16/07

By: _____

Paul P. Kiel
Attorney For Applicant
Registration No. 40,677
609-734-6815

Mailing Address:

Thomson Licensing LLC
PO Box 5312
Princeton, NJ 08543-5312